IN THE CLAIMS:

The following is a current listing of claims and will replace all prior versions and listings of claims in the application. Please amend the claims as follows:

1–104. (Canceled)

105. (Previously Presented) A computer-implemented method comprising:

selecting an active program on a computer system as code under investigation; and

executing malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a first and a second plurality of detection routines, wherein said executing includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results;

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results;

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with malicious code, wherein the second score is obtained independently of the first score; and

using the first and second scores to categorize the code under investigation with respect to the likelihood of the code under investigation compromising the security of the computer system.

106. (Previously Presented) The method of claim 105, wherein the code under investigation has access to other active programs executing on the computer system, and wherein execution of the MCDC does not preclude the selected active code from directly interfacing with an operating system of the computer system.

107. (Previously Presented) The method of claim 105, further comprising:

selecting, in turn, each additional active program on the computer system as code under investigation; and

executing said MCDC with respect to said selected code under investigation.

108. (Canceled)

109. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect remote control software.

110. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect a keystroke logger.

111. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect spyware.

112. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect a worm.

113. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect a virus.

114. (Previously Presented) The method of claim 105, wherein the second plurality of detection routines are configured to detect monitoring software.

115. (Previously Presented) A computer-implemented method comprising:

selecting code currently running on a computer system as code under investigation, wherein said code is running in a manner that permits infection of said computer system; and

executing malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a first and a second plurality of detection routines, wherein said executing includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results;

weighting each of the first plurality of results to obtain a first score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results;

weighting each of the second plurality of results to obtain a second score indicative of whether the code under investigation has characteristics and/or behaviors typically associated with malicious code, wherein the second score is independent of the first score; and

using the first and second scores to categorize the code under investigation into one of a plurality of categories, including first and second categories indicative of valid code and malicious code, respectively.

116. (Previously Presented) The method of claim 115, wherein the code under investigation has access to other active code executing on the computer system.

117. (Previously Presented) The method of claim 115, wherein at least some of the code associated with the selected active code is running in kernel mode.

118. (Previously Presented) The method of claim 115, further comprising:

selecting additional active code as code under investigation; and

executing said MCDC with respect to said selected code under investigation.

119-126. (Canceled)

127. (Previously Presented) A computer system comprising:

a processor; and

a memory storing program instructions executable by the processor to:

select a program currently running on a computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system; and

execute malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a first and a second plurality of detection routines, including:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results;

weighting each of the first plurality of results to obtain a first score indicative of the extent to which the code under investigation has characteristics and/or behaviors typically associated with valid code;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results;

weighting each of the second plurality of results to obtain a second score indicative of the extent to which the code under investigation has characteristics and/or behaviors typically associated with malicious code; and

using the first and second scores to determine whether the code under investigation represents a security threat to the computer system.

128. (Previously Presented) A computer-readable memory medium, including program instructions that are computer executable by a computer system to:

select a program currently running on the computer system as code under investigation, wherein said program is running in a manner that permits infection of said computer system; and

execute malicious code detection code (MCDC) on the computer system, wherein the MCDC includes a first and a second plurality of detection routines, and wherein execution of the MCDC includes:

applying each of the first plurality of detection routines to the code under investigation to obtain a corresponding one of a first plurality of results, wherein the first plurality of detection routines test for characteristics and/or behaviors typically associated with valid code;

weighting and combining each of the first plurality of results to obtain a first composite score;

applying each of the second plurality of detection routines to the code under investigation to obtain a corresponding one of a second plurality of results, wherein the first plurality of detection routines test for characteristics and/or behaviors typically associated with malicious code;

weighting and combining each of the second plurality of results to obtain a second composite score; and

using the first and second scores to determine whether the code under investigation is malicious code.

129. (Previously Presented) The method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is malicious code.

130. (Previously Presented) The method of claim 129, wherein the malicious code does not have a known signature.

131. (Previously Presented) The method of claim 105, wherein the first plurality of detection routines includes routines that examine the behavior of the code under investigation.

132. (Currently Amended) The method of claim 131, wherein the second plurality of detection routines includes routines that examine the behavior of the code under investigation.

133. (Previously Presented) The method of claim 105, wherein the malicious code is a previously unknown type of malicious code.

134. (Previously Presented) The method of claim 129, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

135. (Previously Presented) The method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is valid code.

136. (Previously Presented) The method of claim 135, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value.

137. (Previously Presented) The method of claim 105, further comprising:

determining from the first and second scores that the code under investigation is suspicious code, wherein suspicious code has not been determined to be either valid or malicious code.

138. (Previously Presented) The method of claim 137, wherein the code under investigation is determined to be suspicious code based on the first and second scores being similar.

139. (Previously Presented) The system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is malicious code.

140. (Previously Presented) The system of claim 139, wherein the malicious code is a previously unknown type of malicious code.

141. (Previously Presented) The system of claim 139, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

142. (Previously Presented) The system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is valid code.

143. (Previously Presented) The system of claim 142, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value.

144. (Previously Presented) The system of claim 127, further comprising program instructions executable by the processor to:

determine from the first and second scores that the code under investigation is suspicious code.

145. (Previously Presented) The memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is malicious code.

146. (Previously Presented) The memory medium of claim 145, wherein the malicious code is a previously unknown type of malicious code.

147. (Previously Presented) The memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is valid code.

148. (Previously Presented) The memory medium of claim 147, wherein the determination that the code under investigation is valid code is based on the first score exceeding a valid code threshold value.

149. (Previously Presented) The memory medium of claim 128, further comprising program instructions executable to:

determine from the first and second scores that the code under investigation is suspicious code.

150. (Previously Presented) The memory medium of claim 145, wherein the determination that the code under investigation is malicious code is based on the first score not exceeding a valid code threshold value and the second score exceeding a malicious code threshold value.

151. (Previously Presented) The method of claim 105, wherein at least some of the code associated with the selected active program is running in kernel mode.

152. (Previously Presented) One or more computer-readable media storing program instructions executable on a computer system to:

determine a first value indicative of valid code characteristics and/or behaviors exhibited by a first program running on the computer system;

independently determine a second value indicative of malicious code characteristics and/or behaviors exhibited by the first program;

based on comparisons involving the first and second values, determine whether the first program is a security threat to the computer system.

153. (Previously Presented) The computer-readable media of claim 152, wherein the program instructions are executable to determine whether the first program is a security threat to the computer system based on a first comparison between the first value and a valid code threshold value and also based on a second comparison between the second value and a malicious code threshold value.

154. (Previously Presented) The computer-readable media of claim 152, wherein the program instructions are executable to determine that the first program is a security threat to the computer

system based on the first value not exceeding a valid code threshold value and on the second value exceeding a malicious code threshold value.

155. (Previously Presented) The computer-readable media of claim 152, wherein the program instructions are executable to determine that the first program is not a security threat to the computer system based on the first value exceeding a valid code threshold value.

156. (Previously Presented) The computer-readable media of claim 152, wherein the program instructions are executable to determine that the first program is not a security threat to the computer system based on the first value exceeding a valid code threshold value and on the second value not exceeding a malicious code threshold value.

157. (Previously Presented) The computer-readable media of claim 152, wherein the program instructions are executable to determine that it is unclear whether the first program is a security threat to the computer system based on the first value and the second value not being significantly different from one another.

158. (Previously Presented) The computer-readable media of claim 152, wherein the program instructions are executable to determine that it is unclear whether the first program is a security threat to the computer system based on the first value exceeding a valid code threshold value and the second value exceeding a malicious code threshold value.

159. (Previously Presented) A method, comprising:

computing a first score indicative of valid code characteristics and/or behaviors exhibited by a first program running on a computer system;

computing a second value indicative of malicious code characteristics and/or behaviors exhibited by the first program;

using the first and second values to categorize the first program as to the likelihood of the first program compromising the security of the computer system.

160. (Previously Presented) The method of claim 159, wherein the malicious code characteristics include whether the first program has a signature associated with malicious code.

161. (Previously Presented) The method of claim 159, wherein the malicious code behaviors include whether the first program is performing actions typically associated with one or more types of malicious code.

162. (Previously Presented) The method of claim 159, wherein said using includes performing comparisons involving the first and second values.

163. (Previously Presented) The method of claim 162, wherein said first program is categorized based on a comparison between the first score and a valid code threshold.

164. (Previously Presented) The method of claim 163, wherein the first program is categorized as not being a security threat based on the first score exceeding the valid code threshold.

165. (Previously Presented) The method of claim 162, wherein said first program is categorized based on a comparison between the first score and a valid code threshold and also on a comparison between the second score and a malicious code threshold.

166. (Previously Presented) The method of claim 165, wherein the first program is categorized as not being a security threat based on the first score exceeding the valid code threshold and the second score not exceeding the malicious code threshold.

167. (Previously Presented) A computer system, comprising:

first means for determining a first value indicative of the extent to which a first program running on the computer system has characteristics and/or behaviors typically associated with valid code;

second means for determining a second value indicative of the extent to which the first program has characteristics and/or behaviors typically associated with malicious code;

third means for categorizing, using the first and second values, the first program with respect to whether the first program presents a security threat to the computer system.